

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB10-004

### Vulnerability Summary for the Week of December 28, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activewebsoftwares -- ewebquiz	Multiple SQL injection vulnerabilities in Active Web Softwares eWebquiz 8 allow remote attackers to execute arbitrary SQL commands via the QuizID parameter to (1) questions.asp, (2) importquestions.asp, and (3) quizztakers.asp, different vectors than CVE-2007-1706.	2009-12-28	7.5	<a href="#">CVE-2009-4436</a> XF BID MISC SECUNIA
activewebsoftwares -- active_auction_house	Multiple SQL injection vulnerabilities in Active Auction House 3.6 allow remote attackers to execute arbitrary SQL commands via the (1) catid parameter to wishlist.asp and the (2) linkid parameter to links.asp. NOTE: vector 1 might overlap CVE-2005-1029.1.	2009-12-28	7.5	<a href="#">CVE-2009-4437</a> XF BID MISC SECUNIA MISC
anything-digital -- com_jcalpro	PHP remote file inclusion vulnerability in cal_popup.php in the Anything Digital Development JCal Pro (aka com_jcalpro or JCP) component 1.5.3.6 for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2009-12-28	7.5	<a href="#">CVE-2009-4431</a> BID MISC
	Buffer overflow in the web service in AzeoTech DAQFactory 5.77 might allow remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by a certain module in VulnDisco Pack	2009-12-		<a href="#">CVE-2009-</a>

azeotech -- daqfactory	Professional 7.16 through 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-30	9.3	<a href="#">4480 SECUNIA</a>
codemight -- videocms	SQL injection vulnerability in index.php in CodeMight VideoCMS 3.1 allows remote attackers to execute arbitrary SQL commands via the v parameter in a video action.	2009-12-28	7.5	<a href="#">CVE-2009-4432 MISC SECUNIA MISC</a>
deluxebb -- deluxebb	DeluxeBB 1.3 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain user and configuration information, log data, and gain administrative access via a direct request to scripts in (1) templates/ including (2) templates/deluxe/admincp/, (3) templates/corporate/admincp/, and (4) templates/blue/admincp/; (5) images/; (6) logs/ including (7) logs/cp.php; (8) wysiwyg/; (9) docs/; (10) classes/; (11) lang/; and (12) settings/.	2009-12-30	7.5	<a href="#">CVE-2009-4465 XF XF XF BID MISC</a>
deon_george -- phpldapadmin	Directory traversal vulnerability in cmd.php in phpLDAPAdmin 1.1.0.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the cmd parameter.	2009-12-28	7.5	<a href="#">CVE-2009-4427 BID OSVDB MISC SECUNIA</a>
dvbbs -- dvbbs	SQL injection vulnerability in boardrule.php in DVBBS 2.0 allows remote attackers to execute arbitrary SQL commands via the groupboardid parameter.	2009-12-30	7.5	<a href="#">CVE-2009-4470 BID BUGTRAQ</a>
f3site -- f3site	Multiple directory traversal vulnerabilities in F3Site 2009 allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the GLOBALS[nlang] parameter to (1) mod/poll.php and (2) mod/new.php.	2009-12-28	7.5	<a href="#">CVE-2009-4435 XF BID MISC MISC</a>
freeschool -- freeschool	Multiple PHP remote file inclusion vulnerabilities in FreeSchool 1.1.0 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the CLASSPATH parameter to (1) bib_form.php, (2) bib_pldetails.php, (3) bib_plform.php, (4) bib_plsearchc.php, (5) bib_plsearchs.php, (6) bib_save.php, (7) bib_searchc.php, (8) bib_searchs.php, (9) edi_form.php, (10) edi_save.php, (11) gen_form.php, (12) gen_save.php, (13) lin_form.php, (14) lin_save.php, (15) luo_form.php, (16) luo_save.php, (17) sog_form.php, or (18) sog_save.php in biblioteca/; (19) cal_insert.php, (20) cal_save.php, or (21) cal_saveactivity.php in calendario/; (22) circolari/cir_save.php; or (23) modulistica/mdl_save.php.	2009-12-30	7.5	<a href="#">CVE-2009-4471 XF VUPEN MILWORM SECUNIA</a>
greendesktiny -- green_desktiny	SQL injection vulnerability in news_detail.php in Green Desktiny 2.3.1, and possibly earlier versions, allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-12-29	7.5	<a href="#">CVE-2009-4456 MISC SECUNIA OSVDB</a>
	Stack-based buffer overflow in HAURI ViRobot			

hauri -- virobot_desktop	Desktop 5.5 before 2009-09-28.00 allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by a certain module in VulnDisco Pack Professional 7.15 through 8.11. NOTE: some of these details are obtained from third party information.	2009-12-30	10.0	<a href="#">CVE-2009-4476</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
imotta -- pyrmont_plugin	SQL injection vulnerability in results.php in the Pyrmont plugin 2 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-12-28	7.5	<a href="#">CVE-2009-4424</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
intellicom -- netbiterconfig	Stack-based buffer overflow in NetBiterConfig.exe 1.3.0 in Intellicom NetBiter WebSCADA allows remote attackers to execute arbitrary code via a long hn (hostname) parameter in a crafted HICP-protocol UDP packet.	2009-12-30	10.0	<a href="#">CVE-2009-4462</a> <a href="#">VUPEN</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
intellicom -- netbiter_webscada_firmware intellicom -- netbiter_webscada_ws100 intellicom -- netbiter_webscada_ws200	The firmware for Intellicom NetBiter WebSCADA uses hard-coded passwords, which makes it easier for remote attackers to obtain access.	2009-12-30	10.0	<a href="#">CVE-2009-4463</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
jax_scripts -- jax_guestbook	Jax Guestbook 3.5.0 allows remote attackers to bypass authentication and modify administrator settings via a direct request to admin/guestbook.admin.php.	2009-12-29	7.5	<a href="#">CVE-2009-4447</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
joomlub -- com_joomlub	SQL injection vulnerability in the Joomlub (com_joomlub) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the aid parameter in an auction edit action to index.php.	2009-12-30	7.5	<a href="#">CVE-2009-4475</a> <a href="#">BID</a> <a href="#">MILWoRM</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>
joomplace -- com_joomportfolio	SQL injection vulnerability in the JoomPortfolio (com_joomportfolio) component 1.0.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the secid parameter in a showcat action to index.php.	2009-12-28	7.5	<a href="#">CVE-2009-4428</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MISC</a> <a href="#">OSVDB</a>
mailsite -- mailsite	LDAP3A.exe in MailSite 8.0.4 allows remote attackers to cause a denial of service (heap memory corruption and daemon crash) via unspecified vectors, as demonstrated by a certain module in VulnDisco Pack Professional 7.13 through 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-30	7.8	<a href="#">CVE-2009-4479</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
mikedeboer -- com_zoom	SQL injection vulnerability in the Mike de Boer zoom (com_zoom) component 2.0 for Mambo allows remote attackers to execute arbitrary SQL commands via the catid parameter to index.php.	2009-12-30	7.5	<a href="#">CVE-2009-4474</a> <a href="#">BID</a> <a href="#">MILWoRM</a>
	The prep_reprocess_req function in kdc/do_tgs_req.c			<a href="#">CVE-2009-</a>

mit -- kerberos	in the cross-realm referral implementation in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.7 before 1.7.1 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a ticket request.	2009-12-29	7.8	<a href="#">3295</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">CONFIRM</a>
mysql -- mysql	Buffer overflow in the server in MySQL 5.0.51a on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by the vd_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-30	7.5	<a href="#">CVE-2009-4484</a> <a href="#">MISC</a>
ortro -- ortro	Multiple unspecified vulnerabilities in Ortro before 1.3.4 have unknown impact and attack vectors.	2009-12-31	10.0	<a href="#">CVE-2009-4519</a> <a href="#">XF</a> <a href="#">VUPEN</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
phpope -- phpope	Multiple PHP remote file inclusion vulnerabilities in PhPopo 1.0.0 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the (1) GLOBALS[config][dir][plugins] parameter to plugins/address/admin/index.php, (2) GLOBALS[config][dir][functions] parameter to plugins/im/compose.php, and (3) GLOBALS[config][dir][classes] parameter to plugins/cssedit/admin/index.php.	2009-12-30	7.5	<a href="#">CVE-2009-4472</a> <a href="#">XF</a> <a href="#">VUPEN</a> <a href="#">MILWORM</a>
provider4u -- vsftpd_webmin_module	Multiple unspecified vulnerabilities in the Vsftpd Webmin module before 1.3b for the Vsftpd server have unknown impact and attack vectors related to "Some security issues."	2009-12-29	7.5	<a href="#">CVE-2009-4457</a> <a href="#">VUPEN</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a> <a href="#">CONFIRM</a>
sarg -- squid_analysis_report_generator	Buffer overflow in Squid Analysis Report Generator (Sarg) 2.2.3.1, and probably later, allows user-assisted remote attackers to execute arbitrary code via a long HTTP request method in a crafted access.log file, a different vulnerability than CVE-2008-1167.	2009-12-30	9.3	<a href="#">CVE-2008-7249</a> <a href="#">VUPEN</a> <a href="#">BUGTRAQ</a> <a href="#">CONFIRM</a>
softcab -- sound_converter_activex	Insecure method vulnerability in SoftCab Sound Converter ActiveX control (sndConverter.ocx) 1.2 allows remote attackers to create or overwrite arbitrary files via the SaveFormat method. NOTE: some of these details are obtained from third party information.	2009-12-29	8.8	<a href="#">CVE-2009-4453</a> <a href="#">XF</a> <a href="#">MISC</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
tversity -- tversity	Buffer overflow in MediaServer.exe in TVersity 1.6 allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by the vd_tversity module in VulnDisco Pack Professional 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-30	10.0	<a href="#">CVE-2009-4482</a> <a href="#">MISC</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
virtuemart -- virtuemart	SQL injection vulnerability in index.php in VirtueMart 1.0 allows remote attackers to execute arbitrary SQL commands via the product_id parameter in a	2009-12-28	7.5	<a href="#">CVE-2009-4430</a> <a href="#">BID</a>

	shop.product_details shop.flypage action.			MISC
xstate -- real_estate	SQL injection vulnerability in page.html in Xstate Real Estate 1.0 allows remote attackers to execute arbitrary SQL commands via the pid parameter.	2009-12-30	7.5	CVE-2009-4477 XF MILWoRM SECUNIA OSVDB
zabbix -- zabbix	SQL injection vulnerability in the get_history_lastid function in the nodewatcher component in Zabbix Server before 1.6.8 allows remote attackers to execute arbitrary SQL commands via a crafted request, possibly related to the send_history_last_id function in zabbix_server/trapper/nodehistory.c.	2009-12-31	7.5	CVE-2009-4499 CONFIRM VUPEN BUGTRAQ SECUNIA
zabbix -- zabbix	The NET_TCP_LISTEN function in net.c in Zabbix Agent before 1.6.7, when running on FreeBSD or Solaris, allows remote attackers to bypass the EnableRemoteCommands setting and execute arbitrary commands via shell metacharacters in the argument to net.tcp.listen. NOTE: this attack is limited to attacks from trusted IP addresses.	2009-12-31	9.3	CVE-2009-4502 CONFIRM VUPEN BUGTRAQ SECUNIA

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activewebswares -- active_business_directory	Cross-site scripting (XSS) vulnerability in searchadvance.asp in Active Business Directory 2 allows remote attackers to inject arbitrary web script or HTML via the search parameter.	2009-12-30	4.3	CVE-2009-4464 XF MISC SECUNIA OSVDB
apc -- network_management_card apc -- switched_rack_pdu	Multiple cross-site request forgery (CSRF) vulnerabilities on the Network Management Card (NMC) on American Power Conversion (APC) Switched Rack PDU (aka Rack Mount Power Distribution) devices and other devices allow remote attackers to hijack the authentication of (1) administrator or (2) device users for requests that create new administrative users or have unspecified other impact.	2009-12-28	6.8	CVE-2009-1797 SECUNIA CONFIRM MISC
apc -- network_management_card apc -- switched_rack_pdu	Multiple cross-site scripting (XSS) vulnerabilities on the Network Management Card (NMC) on American Power Conversion (APC) Switched Rack PDU (aka Rack Mount Power Distribution) devices and other devices allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: the login_username vector for Forms/login1 is already covered by CVE-2009-4406.	2009-12-28	4.3	CVE-2009-1798 SECUNIA CONFIRM MISC
bloofox -- bloofoxcms	Cross-site scripting (XSS) vulnerability in search.5.html in BloofoxCMS 0.3.5 allows remote attackers to inject arbitrary web script or HTML via the search parameter to index.php. NOTE: some of these details are obtained from third party information.	2009-12-31	4.3	CVE-2009-4522 XF BID SECUNIA MISC OSVDB
	The default configuration of Cisco ASA 5500 Series			

cisco -- adaptive_security_appliance_5500	Adaptive Security Appliance (Cisco ASA) 7.0, 7.1, 7.2, 8.0, 8.1, and 8.2 allows portal traffic to access arbitrary backend servers, which might allow remote authenticated users to bypass intended access restrictions and access unauthorized web sites via a crafted URL obfuscated with ROT13 and a certain encoding. NOTE: this issue was originally reported as a vulnerability related to lack of restrictions to URLs listed in the Cisco WebVPN bookmark component, but the vendor states that "The bookmark feature is not a security feature."	2009-12-29	6.5	CVE-2009-4455 VUPEN SECTRACK BUGTRAQ CONFIRM SECUNIA OSVDB
deluxebb -- deluxebb	DeluxeBB 1.3 allows remote attackers to obtain sensitive information via a crafted page parameter to misc.php, which reveals the installation path in an error message. NOTE: this issue might be resultant from improperly controlled computation in tools.php that leads to a denial of service (CPU or memory consumption).	2009-12-30	5.0	CVE-2009-4466 XF BID MISC
deluxebb -- deluxebb	misc.php in DeluxeBB 1.3 allows remote attackers to register accounts without a valid email address via a vemail action with the valmem set to a pre-assigned user ID, which is visible from a memberlist action.	2009-12-30	6.5	CVE-2009-4467 XF BID MISC
deluxebb -- deluxebb	Cross-site scripting (XSS) vulnerability in misc.php in DeluxeBB 1.3 allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2009-12-30	4.3	CVE-2009-4468 XF BID MISC
drupal -- storm	The Storm module 6.x before 6.x-1.25 for Drupal does not enforce privilege requirements for storminvoiceitem nodes, which allows remote attackers to read node titles via unspecified vectors.	2009-12-31	5.0	CVE-2009-4515 VUPEN BID SECUNIA CONFIRM CONFIRM
drupal -- faq	Cross-site scripting (XSS) vulnerability in the FAQ Ask module 5.x and 6.x before 6.x-2.0, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-31	4.3	CVE-2009-4516 VUPEN BID SECUNIA CONFIRM
drupal -- faq	Cross-site request forgery (CSRF) vulnerability in the FAQ Ask module 5.x and 6.x before 6.x-2.0, a module for Drupal, allows remote attackers to hijack the authentication of arbitrary users for requests that access unpublished content.	2009-12-31	4.3	CVE-2009-4517 VUPEN SECUNIA CONFIRM
drupal -- insert_node	Cross-site scripting (XSS) vulnerability in the Insert Node module 5.x before 5.x-1.2 for Drupal allows remote attackers to inject arbitrary web script or HTML via an inserted node.	2009-12-31	4.3	CVE-2009-4518 VUPEN BID SECUNIA CONFIRM CONFIRM
drupal -- cck_comment_module	The CCK Comment Reference module 5.x before 5.x-1.2 and 6.x before 6.x-1.3, a module for Drupal, allows remote attackers to bypass intended access restrictions	2009-12-31	5.0	CVE-2009-4520 VUPEN BID

	and read comments by using the autocomplete path.			<b>SECUNIA CONFIRM</b>
drupal -- realname	Cross-site scripting (XSS) vulnerability in the RealName module 6.x-1.x before 6.x-1.3 for Drupal allows remote attackers to inject arbitrary web script or HTML via a realname (aka real name) element.	2009-12-31	4.3	<a href="#">CVE-2009-4524 XF VUPEN BID SECUNIA OSVDB CONFIRM</a>
drupal -- print	Cross-site scripting (XSS) vulnerability in the Print (aka Printer, e-mail and PDF versions) module 5.x before 5.x-4.9 and 6.x before 6.x-1.9, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via crafted data in a list of links.	2009-12-31	4.3	<a href="#">CVE-2009-4525 XF VUPEN BID SECUNIA OSVDB CONFIRM CONFIRM CONFIRM</a>
drupal -- print	The Send by e-mail sub-module in the Print (aka Printer, e-mail and PDF versions) module 5.x before 5.x-4.9 and 6.x before 6.x-1.9, a module for Drupal, does not properly enforce privilege requirements, which allows remote attackers to read page titles by requesting a "Send to friend" form.	2009-12-31	5.0	<a href="#">CVE-2009-4526 VUPEN BID SECUNIA OSVDB CONFIRM CONFIRM CONFIRM</a>
drupal -- organic_groups_vocabulary	The Organic Groups (OG) Vocabulary module 6.x before 6.x-1.0 for Drupal allows remote authenticated group members to bypass intended access restrictions, and create, modify, or read a vocabulary, via unspecified vectors.	2009-12-31	6.5	<a href="#">CVE-2009-4528 XF VUPEN BID SECUNIA OSVDB CONFIRM CONFIRM</a>
drupal -- faq	Open redirect vulnerability in the FAQ Ask module 5.x and 6.x before 6.x-2.0, a module for Drupal, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2009-12-31	4.3	<a href="#">CVE-2009-4534 BID CONFIRM</a>
eclipse -- birt	Cross-site scripting (XSS) vulnerability in birt-viewer/run in Eclipse Business Intelligence and Reporting Tools (BIRT) before 2.5.0, as used in KonaKart and other products, allows remote attackers to inject arbitrary web script or HTML via the _report parameter.	2009-12-31	4.3	<a href="#">CVE-2009-4521 XF</a>
ektron -- cms4000.net	Multiple cross-site scripting (XSS) vulnerabilities in WorkArea/ContentDesigner/ekformsiframe.aspx in Ektron CMS400.NET 7.6.1.53 and 7.6.6.47, and possibly 7.52 through 7.66sp2, allow remote attackers to inject arbitrary web script or HTML via the (1) css, (2) eca, (3) id, and (4) skin parameters. NOTE: some of these details are obtained from third party information.	2009-12-30	4.3	<a href="#">CVE-2009-4473 MISC</a>

flatpress -- flatpress	Multiple cross-site scripting (XSS) vulnerabilities in FlatPress 0.909 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) contact.php, (2) login.php, and (3) search.php.	2009-12-30	4.3	CVE-2009-4461 BID MISC SECUNIA
freepbx -- freepbx	Multiple cross-site scripting (XSS) vulnerabilities in FreePBX 2.5.2 and 2.6.orc2, and possibly other versions, allow remote attackers to inject arbitrary web script or HTML via the (1) tech parameter to admin/admin/config.php during a trunks display action, the (2) description parameter during an Add Zap Channel action, and (3) unspecified vectors during an Add Recordings action.	2009-12-29	4.3	CVE-2009-4458 XF XF BID MISC SECUNIA OSVDB OSVDB
freeradius -- freeradius	Unspecified vulnerability in radiusd in FreeRADIUS 1.1.7 allows remote attackers to cause a denial of service (daemon crash) via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 7.6 through 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-30	5.0	CVE-2009-4481 BID SECUNIA
giombetti -- phppowercards	Multiple cross-site scripting (XSS) vulnerabilities in pagename.inc.php in phpPowerCards 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) PATH_INFO, the (2) archiv parameter, and the (3) subcat parameter.	2009-12-30	4.3	CVE-2009-4469 XF BID MISC
ibm -- db2	The Query Compiler, Rewrite, and Optimizer component in IBM DB2 9.1 before FP8, 9.5 before FP5, and 9.7 before FP1 does not enforce privilege requirements for access to a (1) sequence or (2) global-variable object, which allows remote authenticated users to make use of data via unspecified vectors.	2009-12-28	6.5	CVE-2009-4438 VUPEN CONFIRM
ibm -- db2	Unspecified vulnerability in the Query Compiler, Rewrite, and Optimizer component in IBM DB2 9.5 before FP5 allows remote authenticated users to cause a denial of service (instance crash) by compiling a SQL query.	2009-12-28	4.0	CVE-2009-4439 VUPEN CONFIRM
idevspot -- idevcart	Cross-site scripting (XSS) vulnerability in index.php in iDevCart 1.09 allows remote attackers to inject arbitrary web script or HTML via the SEARCH parameter in a browse action.	2009-12-28	4.3	CVE-2009-4425 XF OSVDB MISC SECUNIA MISC
idevspot -- isupport	Multiple cross-site scripting (XSS) vulnerabilities in IDevSpot iSupport 1.8 and earlier allow remote attackers to inject arbitrary web script or HTML via the (a) 5 or (b) 9 field in a post action to ticket_function.php, reachable through ticket_submit.php and index.php; (c) the which parameter to function.php, or (d) the which parameter to index.php, related to knowledgebase_list.php. NOTE: some of these details are obtained from third party information.	2009-12-28	4.3	CVE-2009-4433 XF XF BID OSVDB OSVDB OSVDB MISC SECUNIA MISC

idevspot -- isupport	Directory traversal vulnerability in index.php in iDevSpot iSupport 1.8 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the include_file parameter.	2009-12-28	5.0	CVE-2009-4434 OSVDB MISC SECUNIA MISC
ikemcg -- phpinstantgallery	Cross-site scripting (XSS) vulnerability in admin.php in phpInstantGallery 1.1 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2009-12-29	4.3	CVE-2009-4446 XF BID MISC
indymedia -- oscailt	Directory traversal vulnerability in index.php in Oscailt 3.3, when Use Friendly URL's is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the obj_id parameter.	2009-12-31	5.1	CVE-2009-4512 XF VUPEN MISC SECUNIA MISC
jazu1oo -- httpdx	httpdx 1.4.4 and earlier allows remote attackers to obtain the source code for a web page by appending a . (dot) character to the URI.	2009-12-31	5.0	CVE-2009-4531 XF OSVDB SECUNIA MISC MISC MISC
kaspersky_lab -- kaspersky_antivirus kaspersky_lab -- kaspersky_antivirus_2009 kaspersky_lab -- kaspersky_antivirus_2010 kaspersky_lab -- kaspersky_antivirus_personal kaspersky_lab -- kaspersky_internet_security kaspersky_lab -- kaspersky_internet_security_2009 kaspersky_lab -- kaspersky_internet_security_2010	Kaspersky Anti-Virus 5.0 (5.0.712); Antivirus Personal 5.0.x; Anti-Virus 6.0 (6.0.3.837), 7 (7.0.1.325), 2009 (8.0.0.x), and 2010 (9.0.0.463); and Internet Security 7 (7.0.1.325), 2009 (8.0.0.x), and 2010 (9.0.0.463); use weak permissions (Everyone:Full Control) for the BASES directory, which allows local users to gain SYSTEM privileges by replacing an executable or DLL with a Trojan horse.	2009-12-29	6.8	CVE-2009-4452 VUPEN SECTRACK SECTRACK BUGTRAQ MISC SECUNIA SECUNIA
launchpad -- ignition	Multiple directory traversal vulnerabilities in Ignition 1.2, when magic_quotes_gpc is disabled, allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the blog parameter to (1) comment.php and (2) view.php.	2009-12-28	6.8	CVE-2009-4426 XF MISC SECUNIA MISC OSVDB OSVDB
livezilla -- livezilla	Multiple cross-site scripting (XSS) vulnerabilities in map.php in LiveZilla 3.1.8.3 allow remote attackers to inject arbitrary web script or HTML via the (1) lat, (2) lng, and (3) zom parameters, which are not properly handled when processed with templates/map.tpl.	2009-12-29	4.3	CVE-2009-4450 BUGTRAQ SECUNIA OSVDB MISC
ljscripts -- auto- surf_traffic_exchange_script	Multiple cross-site scripting (XSS) vulnerabilities in Auto-Surf Traffic Exchange Script 1.1 allow remote attackers to inject arbitrary web script or HTML via	2009-12-29	4.3	CVE-2009-4460 MISC SECUNIA

suri_uronic_exchange_script	the rid parameter to (1) index.php, (2) faq.php, and (3) register.php.	3.0		<a href="#">OSVDB</a> <a href="#">OSVDB</a> <a href="#">OSVDB</a>
mailsite -- mailsite	Unspecified vulnerability in LDAP3A.exe in MailSite 8.0.4 allows remote attackers to cause a denial of service (daemon crash) via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 7.13 through 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-30	5.0	<a href="#">CVE-2009-4483</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
microsoft -- iis	Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp; .jpg file.	2009-12-29	6.0	<a href="#">CVE-2009-4444</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">SECTRACK</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>
microsoft -- iis	Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a : (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.	2009-12-29	6.0	<a href="#">CVE-2009-4445</a> <a href="#">MISC</a> <a href="#">SECTRACK</a>
myboard -- mybb	inc/functions_time.php in MyBB (aka MyBulletinBoard) 1.4.10, and possibly earlier versions, allows remote attackers to cause a denial of service (CPU consumption) via a crafted request with a large year value, which triggers a long loop, as reachable through member.php and possibly other vectors.	2009-12-29	5.0	<a href="#">CVE-2009-4448</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
myboard -- mybb	Directory traversal vulnerability in MyBB (aka MyBulletinBoard) 1.4.10, and possibly earlier versions, when changing the user avatar from the gallery, allows remote authenticated users to determine the existence of files via directory traversal sequences in the avatar and possibly the gallery parameters, related to (1) admin/modules/user/users.php and (2) usercp.php.	2009-12-29	6.3	<a href="#">CVE-2009-4449</a> <a href="#">CONFIRM</a>
nathan_haug -- webform	The Webform module 5.x before 5.x-2.8 and 6.x before 6.x-2.8, a module for Drupal, does not prevent caching of a page that contains token placeholders for a default value, which allows remote attackers to read session variables via unspecified vectors.	2009-12-31	5.0	<a href="#">CVE-2009-4533</a> <a href="#">XF</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2009-</a>

navicopa -- navicopa_web_server	InterVations NaviCOPA Web Server 3.0.1.2 and earlier allows remote attackers to obtain the source code for a web page via a trailing encoded space character in a URI, as demonstrated by /index.html%20 and /index.php%20 URIs.	2009-12-31	5.0	4529 XF VUPEN BID MISC SECUNIA MISC OSVDB MISC	
niif -- shibboleth_authentication_module	The Shibboleth authentication module 5.x before 5.x-3.4 and 6.x before 6.x-3.2, a module for Drupal, does not properly remove statically granted privileges after a logout or other session change, which allows physically proximate attackers to gain privileges by using an unattended web browser.	2009-12-31	4.6	CVE-2009-4527 XF VUPEN BID SECUNIA CONFIRM	
openttd -- openttd	Unspecified vulnerability in the NormaliseTrainConsist function in src/train_cmd.cpp in OpenTTD before 0.7.5-RC1 allows remote attackers to cause a denial of service (daemon crash) via certain game actions involving a wagon and a dual-headed engine.	2009-12-28	5.0	CVE-2009-4007 CONFIRM	
php.html -- kandalf_upper	Unrestricted file upload vulnerability in upper.php in kandalf upper 0.1 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in fileup/.	2009-12-29	6.8	CVE-2009-4451 MISC SECUNIA OSVDB	
redmine -- redmine	Redmine 0.8.7 and earlier uses the title tag before defining the character encoding in a meta tag, which allows remote attackers to conduct cross-site scripting (XSS) attacks and inject arbitrary script via UTF-7 encoded values in the title parameter to a new issue page, which may be interpreted as script by Internet Explorer 7 and 8.	2009-12-30	4.3	CVE-2009-4459 XF BID MISC	
saini -- videocache	vcleaner in VideoCache 1.9.2 allows local users with Squid proxy user privileges to overwrite arbitrary files via a symlink attack on /var/log/videocache/vccleaner.log.	2009-12-29	6.9	CVE-2009-4454 XF BUGTRAQ SECUNIA FULLDISC	
sarg -- squid_analysis_report_generator	Cross-site scripting (XSS) vulnerability in Squid Analysis Report Generator (Sarg) 2.2.4 allows remote attackers to inject arbitrary web script or HTML via a JavaScript onload event in the User-Agent header, which is not properly handled when displaying the Squid proxy log. NOTE: this issue exists because of an incomplete fix for CVE-2008-1168.	2009-12-30	4.3	CVE-2008-7250 VUPEN CONFIRM SECUNIA	
sun -- java_system_directory_server	Directory Proxy Server (DPS) in Sun Java System Directory Server Enterprise Edition 6.0 through 6.3.1 does not properly handle multiple client connections within a short time window, which allows remote attackers to hijack the backend connection of an authenticated user, and obtain the privileges of this user, by making a client connection in opportunistic circumstances, related to "long binds," aka Bug Ids 6828462 and 6823593.	2009-12-28	6.8	CVE-2009-4440 SUNALERT CONFIRM	
	Directory Proxy Server (DPS) in Sun Java System				

sun -- java_system_directory_server	Directory Server Enterprise Edition 6.0 through 6.3.1 does not enable the SO_KEEPALIVE socket option, which makes it easier for remote attackers to cause a denial of service (connection slot exhaustion) via multiple connections, aka Bug Id 6782659.	2009-12-28	5.0	CVE-2009-4441 SUNALERT CONFIRM
sun -- java_system_directory_server	Directory Proxy Server (DPS) in Sun Java System Directory Server Enterprise Edition 6.0 through 6.3.1 does not properly implement the max-client-connections configuration setting, which allows remote attackers to cause a denial of service (connection slot exhaustion) by making multiple connections and performing no operations on these connections, aka Bug Id 6648665.	2009-12-28	5.0	CVE-2009-4442 SUNALERT CONFIRM
sun -- java_system_directory_server	Unspecified vulnerability in the psearch (aka persistent search) functionality in Directory Proxy Server (DPS) in Sun Java System Directory Server Enterprise Edition 6.0 through 6.3.1 allows remote attackers to cause a denial of service (psearch outage) by using a crafted psearch client to send requests that trigger a psearch thread loop, aka Bug Id 6855978.	2009-12-28	4.3	CVE-2009-4443 SUNALERT CONFIRM
valenok -- mongoose	Mongoose 2.8.0 and earlier allows remote attackers to obtain the source code for a web page by appending ::\$DATA to the URI.	2009-12-31	5.0	CVE-2009-4530 SECUNIA MISC
valenok -- mongoose	Mongoose 2.8.0 and earlier allows remote attackers to obtain the source code for a web page by appending a / (slash) character to the URI.	2009-12-31	5.0	CVE-2009-4535 SECUNIA MISC MISC
xstate -- real_estate	Multiple cross-site scripting (XSS) vulnerabilities in Xstate Real Estate 1.0 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) home.html or (2) lands.html.	2009-12-30	4.3	CVE-2009-4478 XF MILWoRM SECUNIA OSVDB OSVDB
zabbix -- zabbix	The node_process_command function in Zabbix Server before 1.8 allows remote attackers to execute arbitrary commands via a crafted request.	2009-12-31	6.8	CVE-2009-4498 CONFIRM VUPEN BUGTRAQ SECUNIA
zabbix -- zabbix	The process_trap function in trapper/trapper.c in Zabbix Server before 1.6.6 allows remote attackers to cause a denial of service (crash) via a crafted request with data that lacks an expected : (colon) separator, which triggers a NULL pointer dereference.	2009-12-31	5.0	CVE-2009-4500 CONFIRM VUPEN BUGTRAQ SECUNIA
zabbix -- zabbix	The zbx_get_next_field function in libs/zbxcommon/str.c in Zabbix Server before 1.6.8 allows remote attackers to cause a denial of service (crash) via a request that lacks expected separators, which triggers a NULL pointer dereference, as demonstrated using the Command keyword.	2009-12-31	5.0	CVE-2009-4501 CONFIRM VUPEN BUGTRAQ SECUNIA
zainu -- zainu	Cross-site scripting (XSS) vulnerability in index.php in Zainu 1.0 allows remote attackers to inject arbitrary	2009-12-31	5.0	CVE-2009-4523 XF

<a href="#">zannu -- zannu</a>	web script or HTML via the searchSongKeyword parameter in a SearchSong action.	31	4.3	<a href="#">BID</a> <a href="#">MISC</a> <a href="#">SECUNIA</a>
--------------------------------	--	----	-----	--

[Back to top](#)

<b>Low Vulnerabilities</b>				
<b>Primary Vendor -- Product</b>	<b>Description</b>	<b>Published</b>	<b>CVSS Score</b>	<b>Source &amp; Patch Info</b>
alexander_hass -- sections_module	Cross-site scripting (XSS) vulnerability in the Sections module 5.x before 5.x-1.3 and 6.x before 6.x-1.3 for Drupal allows remote authenticated users with "administer sections" privileges to inject arbitrary web script or HTML via a section name (aka the Name field).	2009-12-28	3.5	<a href="#">CVE-2009-4429</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
drupal -- workflow	Multiple cross-site scripting (XSS) vulnerabilities in the Workflow module 5.x before 5.x-2.4 and 6.x before 6.x-1.2, a module for Drupal, allow remote authenticated users, with "administer workflow" privileges, to inject arbitrary web script or HTML via the name of a (1) workflow or (2) workflow state.	2009-12-31	3.5	<a href="#">CVE-2009-4513</a> <a href="#">XF</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
drupal -- shindig-integrator	Cross-site scripting (XSS) vulnerability in the OpenSocial Shindig-Integrator module 5.x and 6.x before 6.x-2.1, a module for Drupal, allows remote authenticated users, with "create application" privileges, to inject arbitrary web script or HTML via unspecified vectors.	2009-12-31	3.5	<a href="#">CVE-2009-4514</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
nathan_haug -- webform	Cross-site scripting (XSS) vulnerability in the Webform module 5.x before 5.x-2.8 and 6.x before 6.x-2.8, a module for Drupal, allows remote authenticated users, with webform creation privileges, to inject arbitrary web script or HTML via a field label.	2009-12-31	3.5	<a href="#">CVE-2009-4532</a> <a href="#">XF</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a> <a href="#">CONFIRM</a>

[Back to top](#)

Last updated January 04, 2010

 Print This Document